Power semigroups and two rigidity theorems for groups

Salvatore TRINGALI[1]

The Open Seminar

School of Mathematical Sciences, Hebei Normal University
Shijiazhuang, China · June 11, 2026

[1] Based on joint work with Shuolin Liu (School of Mathematical Sciences, HebNU)

Outline

Power semigroups and power monoids

Throughout, every sgrp will be written multiplicatively
and identified with its underlying set, unless stated otherwise.

The large power semigroup of a sgrp H is the sgrp $\mathcal{P}(H)$ obtained by endowing the *non-empty* subsets of H with the (provably associative) operation

$$(X, Y) \mapsto XY := \{xy \colon x \in X,\, y \in Y\}.$$

Moreover, the non-empty *finite* subsets of H form a subsgrp of $\mathcal{P}(H)$, denoted by $\mathcal{P}_{\rm fin}(H)$ and called the finitary power semigroup of H.

If, in particular, H is a monoid with identity 1_H, then $\mathcal{P}(H)$ and $\mathcal{P}_{\rm fin}(H)$ are themselves monoids with identity $\{1_H\}$, and we refer to them as the large power monoid and as the finitary power monoid of H, resp.

Altogether, these structures will be referred to as power semigroups (power sgrps) or power monoids (PMs), depending on the situation.

If the semigroup H is written additively, we adopt the same convention for any subsemigroup of $\mathcal{P}(H)$, so that the operation on $\mathcal{P}(H)$ becomes

$$(X, Y) \mapsto X + Y := \{x + y : x \in X,\, y \in Y\}.$$

Recent literature and popularization

Power sgrps went "dormant" for about 20 years and were rediscovered in 2018:

- Fan & T., J. Algebra **512** (2018), 252–294.

The paper has brought new life to the topic, leading to the following pubs:

- Antoniou & T., Pacific J. Math. **312** (2021), No. 2, 279–308.
- T., J. Algebra **602** (July 2022), 352–380 (Sect. 4.2).
- Bienvenu & Geroldinger, Israel J. Math. **265** (2025), 867–900.
- T. & Yan, Proc. AMS **153** (2025), No. 3, 913–919.
- T. & Yan, J. Comb. Theory Ser. A **209** (2025), #105961, 16 pp.
- García-Sánchez & T., Proc. AMS (2025), No. 6, 2323–2339.
- Cossu & T., J. Algebra **686** (Jan 2026), 793–813.
- Rago, Proc. Amer. Math. Soc. **154** (2026), 1855–1858.
- T. & Yan, Bull. London Math. Soc., to appear (2026).
- T., Amer. Math. Monthly, to appear (2026).
- T. & Wen, Trans. London Math. Soc. **13** (2026), paper No. e70030.

The list is far from complete. For a thorough review of the literature, see

`https://salvo-tringali.github.io/home/biblio-on-power-semigroups.html`

Why caring?

1) A natural algebraic framework for Additive NT and related fields:

- **Sárközy's conjecture**[(2)]**.** For all but finitely many primes p, the set of [non-zero] squares of a finite field $\mathbb{F}$ of order p is an atom[(3)] in the finitary power sgrp of $(\mathbb{F}, +)$.
- **Ostmann's conjecture**[(4)]**.** Every set of integers that differ from the set of primes by finitely many elements is an atom in the large power sgrp of $(\mathbb{Z}, +)$.

2) A leading example in the development of an *extended theory of factorization*:

- T., J. Algebra **602** (July 2022), 352–380.
- Cossu & T., Israel J. Math. **263** (2024), 349–395.
- Cossu & T., J. Algebra **630** (2023), 128–161.
- T., Math. Proc. Cambridge Philos. Soc. **175** (2023), 459-465.
- Casabella, García-Sánchez, & D'Anna, Mediterr. J. Math. **21** (2024), #7, 28 pp.
- Cossu & T., J. Algebra **686** (2026), 793-813.
- [Preprints] Ajran & Gotti (`arXiv:2305.00413`).

3) A key role in the study of formal languages and automata[(5)].

---

(2) Conjecture 1.6 in [Sárközy, Acta Arith. **155** (2012), No. 1, 41–51].
(3) An atom of a monoid M is a non-unit $a \in M$ s.t. $a \neq bc$ for all non-units $b, c \in M$.
(4) Proof announced by Kalmynin in `https://arxiv.org/abs/2504.10202`.
(5) See (the refs in) [Auinger & Steinberg, Theoret. Comput. Sci. **341** (2005), 1–21].

Outline

A dive into the past

A milestone in the study of power sgrps was marked by a 1967 paper of Tamura and Shafer[(6)] that has eventually led to the following:

Problem 1.

Let $\mathcal{O}$ be a class of sgrps. Is it true that, for all $H, K \in \mathcal{O}$,

(1) $\mathcal{P}(H)$ is isomorphic to $\mathcal{P}(K)$ if and only if H is isomorphic to K?

(2) $\mathcal{P}_{\rm fin}(H)$ is isomorphic to $\mathcal{P}_{\rm fin}(K)$ if and only if H is isomorphic to K?

Problem 1(1) is often stated in the equivalent form:

Two semigroups in the class $\mathcal{O}$ are globally isomorphic iff they are isomorphic.

Here, we say that two semigroups H and K are globally isomorphic if there is a global isomorphism from H to K, that is, an isomorphism from $\mathcal{P}(H)$ to $\mathcal{P}(K)$.

The terminology is motivated by the fact that, especially in earlier literature, the large power sgrp of a sgrp H was also referred to as the global of H.

(6) Tamura and Shafer, *Power semigroups*, Math. Japon. **12** (1967), 25–32.

The Tamura–Shafer problem

Problem 1(1) is commonly known as the Tamura–Shafer problem.

It was quickly answered in the negative for *arbitrary* sgrps[7], but has a positive answer in many significant cases (the list is *not* complete):

- groups [Shafer, Math. Japon. **12** (1967), 32].
- semilattices, see p. 218 in [Kobayashi, Semigroup Forum **29** (1984), 217–222].
- completely 0-simple sgrps and completely simple sgrps, see Theorems 5.9 and 6.8 in [Tamura, J. Algebra **98** (1986), 319–361].
- Clifford sgrps, see Theorem 4.7 in [Gan & Zhao, J. Aust. Math. Soc. **97** (2014), 63–77].

The problem is open, e.g., for *finite* sgrps and *cancellative*[8] sgrps.

T. has solved it in a stronger version in the cancellative *commutative* setting, both in its original form and in the variant for finitary power sgrps [T., 2024]

This latter result has been further generalized to the cancellative *duo* setting [Li & T., 202?], where a sgrp H is duo if $aH = Ha$ for all $a \in H$.

(7) See [Mogiljanskaja, Semigroup Forum **6** (1973), 330–333]. Note, however, that the problem has a very simple negative answer in an axiomatic system where GCH doesn't hold.

(8) A sgrp S is cancellative if $x \mapsto ax$ and $x \mapsto xa$ are injective fncs on S for every $a \in S$.

In & Out

Problem1(2) is new (very little is known): it is implicitly addressed in

- T., "On the isomorphism problem for power semigroups", pp. 429–437: M. Brear, A. Geroldinger, B. Olberding, & D. Smertnig (eds.), *Recent Progress in Ring and Factorization Theory*, Springer Proc. Math. Stat. **477**, Springer, 2025;

and it is explicitly stated as Question 4(1) in

- García–Sánchez & T., Proc. Amer. Math. Soc. **153** (2025), 2323–2339.

Problems 1(1) and 1(2) are both trivial in the "if" direction. Indeed, if $f\colon H \to K$ is a sgrp homomorphism, then its augmentation

$$f^*\colon \mathcal{P}(H) \to \mathcal{P}(K)\colon X \mapsto f[X] := \{f(x) : x \in X\} \tag{1}$$

is also a sgrp homomorphism. Moreover, f is injective (resp., surjective) iff so is f^*, and $f^*(X)$ is a (non-empty) finite subset of K for every $X \in \mathcal{P}_{\text{fin}}(H)$.

Since a sgrp S naturally embeds into $\mathcal{P}_{\text{fin}}(S)$ via $x \mapsto \{x\}$, this means that every sgrp isomorphism canonically extends to a global isomorphism, which in turn "restricts" to an isomorphism of the corresponding finitary power sgrps.

An isomorphism between power sgrps arising in this way is called inner (or, in older terminology, a standard isomorphism); otherwise, it is called outer.

Power functors

From Slide 9, there is a well-defined endofunctor $\mathcal{P}$ (resp., $\mathcal{P}_{\rm fin}$) of the category Sgrp of sgrps and sgrp homomorphisms that maps a sgrp to its large (resp., finitary) power sgrp and a sgrp homomorphism f to its augmentation f^* (resp., to the restriction of f^* to finite sets).

This naturally leads to the following generalization of Problem 1:

Problem 2 (Functorial Isomorphism Problem or FIP).

Given a ("reasonable") functor $F\colon \mathcal{C} \to \mathcal{D}$ and a class $\mathcal{O} \subseteq \mathrm{Ob}(\mathcal{C})$, prove or disprove that $F(A) \cong_{\mathcal{D}} F(B)$, for arbitrary $A, B \in \mathcal{O}$, iff $A \cong_{\mathcal{C}} B$, where $\cong_{\mathcal{C}}$ (resp., $\cong_{\mathcal{D}}$) denotes isomorphism in $\mathcal{C}$ (resp., in $\mathcal{D}$).

Instances of the FIP can be found in virtually every area of mathematics:

- Higman's isomorphism problem for groups rings;
- rigidity problems in topology;
- reconstruction problems in graph theory;
- ...

Outline

Global closedness

We mentioned on Slide 8 that, back in 1967, Shafer proved that the Tamura–Shafer problem has a positive answer for groups.

However, the answer to the following question (arising from an Oct 2012 post on MathOverflow) appears to have been unknown until recently:

Problem 3.

If a group H is globally isomorphic to a sgrp K, then is K necessarily a group?

This is an instance of a much more general problem, which is, once again, most naturally formulated in the language of categories:

Problem 4 (Functorial closure problem or FCP).

Given a functor $F\colon \mathcal{C} \to \mathcal{D}$ and a class $\mathcal{O} \subseteq \mathrm{Ob}(\mathcal{C})$ closed under isomorphisms, does $F(A) \simeq_{\mathcal{D}} F(B)$ with $A \in \mathcal{O}$ and $B \in \mathrm{Ob}(\mathcal{C})$ imply $B \in \mathcal{O}$?

If the last problem has a positive answer, the class $\mathcal{O}$ is called F-closed.

In particular, we say that a class of sgrps is globally closed if it is $\mathcal{P}$-closed, where $\mathcal{P}$ is the large-power-sgrp functor from Slide 10.

Unit-invariance

For instance, the following classes of sgrps are globally closed:

(1) The class of all sgrps (obvious and uninteresting).

(2) Finite sgrps (if two sgrps are globally isomorphic, their power sets are equipotent).

(3) Commutative sgrps (a simple exercise).

(4) Monoids (Lemma 1.1 in [Gould et al., Algebra Universalis **19** (1984), 137–141]).

It turns out that groups are also globally closed, that is, the answer to Problem 3 is in the positive. Crucial to the proof is the following:

Definition.

Given a monoid M, we say that an element $x \in M$ is unit-invariant if $ux = x = xu$ for all $u \in M^\times$ (where $M^\times$ is the group of units of M).

The following lemma is straightforward from the definitions:

Lemma.

A sgrp isomorphism from a monoid H to a monoid K maps unit-invariant elements of H to unit-invariant elements of K.

Groups are globally closed

In hindsight, proving that groups are globally closed is not at all difficult. One key (and well-known) observation is that the units of the large PM of a monoid M are precisely the singletons $\{u\}$ with $u \in M^\times$, which implies in turn that

$$X \in \mathcal{P}(M) \text{ is unit-invariant iff } XM^\times = M^\times X = X.$$

This leads to the following:

Theorem 1 (Liu & T. · 202?).

If f is a global iso from a monoid H to a monoid K, then f maps $H^\times$ to $K^\times$ and hence restricts to a global isomorphism from $H^\times$ to $K^\times$.

From here, it is quite easy to conclude:

Proof that groups are globally closed.

Let f be a global iso from a group H to a sgrp K. Since the class of monoids is globally closed (Slide 13), K is a monoid. It follows that f restricts to a global iso from $H^\times$ to $K^\times$ (Theorem 1) and is therefore an iso $\mathcal{P}(H) \to \mathcal{P}(K^\times)$. Since $\mathcal{P}(K^\times)$ is contained in $\mathcal{P}(K)$ and, by hp, f is also an iso $\mathcal{P}(H) \to \mathcal{P}(K)$, this is only possible if $K^\times = K$. ∎

And after the appetizer. . .

Groups are cancellative semigroups. So, looking for generalizations of the previous result (on the global closedness of groups) has eventually led to:

Conjecture

The class of cancellative sgrps is globally closed.

The conjecture is already challenging for *very* special classes of (cancellative) sgrps, as I hope to convince you by outlining the proof of the following:

Theorem 2 (Li & T. · 202?).

Numerical monoids are globally closed.

By Corollary 1 in [Tri-2025] (Slide 9), two cancellative *commutative* sgrps are globally isomorphic iff they are isomorphic.

Theorem 2 is thus reduced to demonstrating that a numerical monoid can only be globally isomorphic to a cancellative commutative sgrp.

This requires a lot of creative ideas and relies on structural results borrowed from Additive Combinatorics (does there exist a more direct proof?).

Proof of Theorem 2 (breakdown)

STEP 1: Given a monoid M and a subset X of M containing 1_M, show that the equation $AX = X^3$ has finitely many solutions A in $\mathcal{P}(M)$ iff X is finite.

STEP 2: Show that if a numerical monoid H is globally iso to a monoid K, then K is torsion-free (i.e., if $1_K \neq x \in K$, then $x, x^2, \ldots$ are pairwise distinct).

STEP 3: Deduce from STEPS 1 and 2 that if f is a global isomorphism from H to K, then for every $y \in K$ there exists $x \in H$ s.t. $f^{-1}(\{1_K, y\}) = \{0, x\}$.

STEP 4: Use STEPS 2 and 3 to prove that $x^2 \neq xy$ for all $x, y \in K$ with $x \neq y$.

STEP 5: Note that K is a fortiori a commutative monoid, and suppose for a contradiction that K is not cancellative, which is tantamount to having that $x\{1_K, y\} = x\{1_K, z\}$ for some $x, y, z \in K$ with $xy = xz$ and $y \neq z$.

STEP 6: Setting $X := f^{-1}(\{x\})$ and $X' := X - \min X$, this leads, by STEP 3, to $X' + \{0, u\} = X' + \{0, v\}$, where $u, v \in \mathbb{N}$ and $u \neq v$.

STEP 7: From STEP 6, the lower asymptotic density of X' is positive and hence, by a classical thm of Kneser, $2nX = nX + n \min X$ for some $n \in \mathbb{N}^+$.

STEP 8: Denote by a the (provably) unique element in $f(\{\min X\})$ and conclude from STEPS 4 and 7 that $x^n = a^n$, which is impossible because a^n is a cancellative element of K, but x^n is not.

Outline

Why the finitary case is different

Having shown that the class of groups is closed under the functor $\mathcal{P}$, it is natural to ask whether the same conclusion remains valid for its finitary counterpart $\mathcal{P}_{\mathrm{fin}}$. This leads to the following:

Problem 5.

Let H be a group. Prove or disprove that, if $\mathcal{P}_{\mathrm{fin}}(H) \cong \mathcal{P}_{\mathrm{fin}}(K)$ for an arbitrary semigroup K, then K is itself a group, and hence $H \cong K$.

The argument used in the "large setting" relies critically on the fact that

$$H^\times \in \mathcal{P}(H).$$

However, if H is an *infinite* group, then $H^\times = H \notin \mathcal{P}_{\mathrm{fin}}(H)$. So we ask:

Problem 6.

Given an isomorphism $f\colon \mathcal{P}_{\mathrm{fin}}(H) \to \mathcal{P}_{\mathrm{fin}}(K)$ between monoids, must f restrict to an isomorphism $\mathcal{P}_{\mathrm{fin}}(H^\times) \to \mathcal{P}_{\mathrm{fin}}(K^\times)$?

This seems to make Problem 5 much more complicated than in the large setting, and we will only solve it here in the special (but fundamental) case where H is a subgroup of $(\mathbb{Q}, +)$.

Let's bring it to order!

Our starting point is to understand, more generally, what happens with a group H that comes endowed with a *total* order $\preceq$ such that

$$\text{if } x \preceq y, \text{ then } uxv \preceq uyv \text{ for all } u, v \in H.$$

In this setting, we can naturally define a surjection

$$\mu \colon \mathcal{P}_{\text{fin}}(H) \to H$$

by mapping a non-empty finite $X \subseteq H$ to its $\preceq$-minimum, that is, the unique $m_X \in X$ s.t. $m_X \preceq x$ for all $x \in X$. Since

$$\mu(XY) = \mu(X)\mu(Y), \qquad \text{for all } X, Y \in \mathcal{P}_{\text{fin}}(H),$$

the map μ is a homomorphism; we call it the minimizer of $(H, \preceq)$.

Proposition 1 (Liu & T. · 202?).

If $(H, \preceq)$ is a totally ordered *abelian* group and $\mathcal{P}_{\text{fin}}(H)$ is isomorphic to $\mathcal{P}_{\text{fin}}(K)$ for a certain semigroup K, then there exists a submonoid L of K s.t.

$$L^\times = \{1_K\} \quad \text{and} \quad K \cong L \times K^\times \cong L \times H.$$

What remains to prove is that the "residual factor" L is trivial.

Fibonacci's rabbits

Given a monoid H and a non-torsion $a \in H$, we may consider the equation

$$\{1_H, a\}X = \{1_H, a\}^n \tag{2}$$

in the unknown $X \in \mathcal{P}(H)$ and the parameter $n \in \mathbb{N}$. Somewhat surprisingly:

Proposition 2 (Liu & T. · 202?).

Equation (2) has exactly F_n solutions X, where F_n is the n-th Fibonacci number (that is, $F_0 := 0$, $F_1 := 1$, and $F_n := F_{n-1} + F_{n-2}$ for $n \geq 2$). Moreover, every solution is finite and contains 1_H.

The point is that, after identifying the cyclic submonoid of H generated by a with $(\mathbb{N}, +)$, we are reduced to consider the "equivalent equation"

$$\{0, 1\} + Y = [\![0, n]\!],$$

over the finitary power monoid of $(\mathbb{N}, +)$. It is then easily seen that, for $n \geq 1$,

$$\{0, n-1\} \subseteq Y \subseteq [\![0, n-1]\!].$$

Moreover, for each $i \in [\![1, n-2]\!]$, at least one of $i-1$ and i must belong to Y. Equivalently, the complement of Y in $[\![1, n-2]\!]$ contains no two consecutive integers, and this is how the Fibonacci sequence pops up in the end!

Indexed signed binary representations

Let an indexed signed binary representation be any sum over $\mathbb{Z}$ of the form

$$2^{e_1}\varepsilon_1 + \cdots + 2^{e_r}\varepsilon_r,$$

where

- the coefficients ε_i are either 1 or -1;
- the exponents e_i are non-negative integers (they need not be distinct);
- the non-negative integer r is called the length of the representation.

Using a deep result of Evertse, Schlickewei, and Schmidt[9] on S-unit equations, it is now possible to prove the following:

Proposition 3 (cf. Bérczes, Hajdu, Pink, & Rout · JNT 2019).

The Fibonacci numbers do not admit indexed signed binary representations of uniformly bounded length for infinitely many indices.

This is the number-theoretic obstruction that will force L in Proposition 1 to be trivial in the special case where H is an additive subgroup of $\mathbb{Q}$.

(9) Ann. of Math. (2) **155** (2002), no. 3, 807–836.

Fibering

The last ingredient in our proof is a bound for the fibers of setwise multiplication in an arbitrary semigroup.

Proposition 4 (Liu & Tringali · 202?).

Let A and B be non-empty *finite* subsets of a semigroup H, and let $\mathcal{S}$ be the set of all $Y \in \mathcal{P}_{\text{fin}}(H)$ such that $AY = B$. If $\mathcal{S}$ is finite, then $|\mathcal{S}|$ has an indexed signed binary representation of length at most $2^{|B|}$.

The idea of the proof is quite simple: describe the solutions Y as subsets of a finite ambient set and apply inclusion–exclusion.

This is then combined with the following lemma, which is the only place where we need H to be an additive subgroup of $\mathbb{Q}$:

Lemma (Liu & Tringali · 202?).

Let H be an additive subgroup of the rational numbers, and let f be an isomorphism from $\mathcal{P}_{\text{fin}}(H)$ to the finitary power semigroup $\mathcal{P}_{\text{fin}}(K)$ of a semigroup K. If K is *not* a group, there exist a positive element $q \in H$ and an integer $N \geq 1$ such that the size of the set $f(\{0, q\})^n$ is bounded by N for infinitely many $n \in \mathbb{N}^+$.

The contradiction mechanism

Assume, for a contradiction, that H is an additive subgroup of $\mathbb{Q}$ and the residual factor L in Proposition 1 is non-trivial.

By the previous lemma, there exist $q \in H^+$ and $N \in \mathbb{N}^+$ such that

$$\left|f(\{0,q\})^n\right| \le N \tag{3}$$

for infinitely many n. Let $B := f(\{0,q\})$ and count the solutions Y of

$$BY = B^n \tag{4}$$

over $\mathcal{P}_{\rm fin}(K)$. Applying f^{-1} turns this into

$$\{0,q\} + X = n\{0,q\}.$$

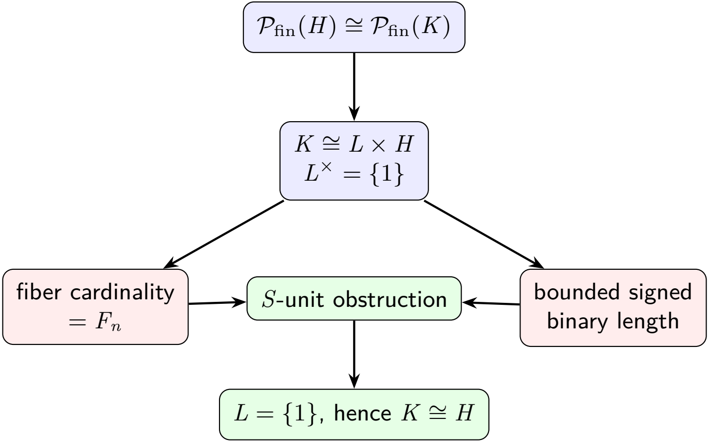
By Proposition 2, the number of solutions is therefore F_n.

Consequently, the fiber bound (Proposition 4) applied to Eq. (4) yields, by Eq. (3), an indexed signed binary representation of F_n of length at most

$$2^{|B^n|} \le 2^N$$

for infinitely many n. However, this is in contradiction with Proposition 3.

A selfie of the proof



Outline

Open problems

Question (A).

Let H be a group and K a semigroup. Does

$$\mathcal{P}_{\mathrm{fin}}(H) \cong \mathcal{P}_{\mathrm{fin}}(K)$$

always imply $H \cong K$?

A natural first step is the case of torsion-free abelian groups. Theorem B settles the rank-one rational case where H is a subgroup of $(\mathbb{Q}, +)$.

Question (B).

Assume H and K are monoids. Does every isomorphism

$$f\colon \mathcal{P}_{\mathrm{fin}}(H) \to \mathcal{P}_{\mathrm{fin}}(K)$$

restrict to an isomorphism

$$f_{\mathrm{fin}}\colon \mathcal{P}_{\mathrm{fin}}(H^\times) \to \mathcal{P}_{\mathrm{fin}}(K^\times),$$

meaning that $f(X) \subseteq K^\times$ for every non-empty finite $X \subseteq H^\times$?

References

- A. A. Antoniou & S. Tringali, *On the Arithmetic of Power Monoids and Sumsets in Cyclic Groups*, Pacific J. Math. **312** (2021), No. 2, 279–308 (arXiv:1804.10913).
- P.-Y. Bienvenu & A. Geroldinger, *On algebraic properties of power monoids of numerical monoids*, Israel J. Math. **265** (2025), 867–900 (arXiv:2205.00982).
- Y. Fan & S. Tringali, *Power monoids: A bridge between Factorization Theory and Arithmetic Combinatorics*, J. Algebra **512** (2018), 252–294 (arXiv:1701.09152).
- P. A. García-Sánchez & S. Tringali, *Semigroups of ideals and isomorphism problems*, Proc. Amer. Math. Soc. **153** (2025), No. 6, 2323–2339.
- L. Li & S. Tringali, *On global isomorphisms and a closure property of semigroups*, preprint (arXiv:2510.00772).
- S. Tringali, *An abstract factorization theorem and some applications*, J. Algebra **602** (July 2022), 352–380 (arXiv:2102.01598).
- S. Tringali, "On the isomorphism problem for power semigroups", pp. 429–437 in: M. Brešar, A. Geroldinger, B. Olberding, and D. Smertnig (eds.), *Recent Progress in Ring and Factorization Theory*, Springer Proc. Math. Stat. **477**, Springer, 2025 (arXiv:2402.11475).
- S. Tringali & K. Wen, *The automorphism group of the finitary power monoid of the integer under addition*, preprint (arXiv:2504.12566).
- S. Tringali & W. Yan, *A conjecture by Bienvenu and Geroldinger on power monoids*, Proc. Amer. Math. Soc. **153** (2025), 913–919 (arXiv:2310.17713).
- S. Tringali & W. Yan, *On power monoids and their automorphisms*, J. Comb. Theory Ser. A **209** (2025), #105961, 16 pp. (arXiv:2312.04439).